6

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,223	08/16/2001	Thomer Michael Gil	12221-007001	2855

26161 7590 07/03/2007

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
NAWAZ, ASAD M	
ART UNIT	PAPER NUMBER
2155	
MAIL DATE	DELIVERY MODE
07/03/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/931,223
Filing Date: August 16, 2001
Appellant(s): GIL ET AL.

Mazu Networks, Inc.
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 4/4/07 appealing from the Office action mailed 6/6/06.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Lyle et al (USPN 6,971,028) hereinafter referred to as Lyle published 11/29/2005.

Hsu et al (USPN: 6,098,157) hereinafter referred to as Hsu published 8/1/2001.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 63-68 and 70-75 rejected under 35 U.S.C. 102(e) as being anticipated by Lyle et al (USPN: 6,971,028) hereinafter referred to as Lyle.

As to claim 63, Lyle teaches a method of monitoring traffic flow in a monitor device disposed to receive network traffic packets comprises:

Producing statistics corresponding to a parameter of traffic flow to trace the source of an attack (Fig 9, 908-310; col 2, lines 45-50; col 7, lines 3-12; sniffers are used in analyzing and evaluating traffic flows to scrutinize suspicious activity in an attempt to ascertain the source of an attack), with producing further comprising:

Mapping the traffic flow into a plurality of buckets (col 7, lines 43-67; event data, which is defined as suspicious data is placed in a queue as a set corresponding to a single incident)

Varying the number of buckets according to the amount of traffic and number of flows according to down traffic flow into different buckets and examining statistics

accumulated for a parameter and a corresponding threshold in the bucket (col 7, line 43 to col 8, line 5; col 13, lines 42-50; once an event (a set of data corresponding to an attack) is placed in the queue, other event data is grouped or combined with existing event data to associate related events into a single incident object. Also, events that do not bear similarities on their face may also be combined or aggregated based upon event rate in a given network or sub-network. Thus varying the amount of event data sets destined for the analysis framework module).

As to claim 64, Lyle teaches the method of claim 63 wherein varying varies the number of buckets so that the monitoring device is not vulnerable to DoS attacks against its own resources (col 19, lines 37-45; the protocol disclosed by Lyle teaches a strong protection against denial of service attacks as well as other forms of attacks).

As to claim 65, Lyle teaches the method of claim 63 wherein varying the number of buckets comprises: comparing the number of buckets to a threshold number of buckets, determining whether the number of buckets should be divided into more buckets or combined into fewer buckets based on comparing the number of buckets to the threshold and as the number of buckets changes, the buckets have values derived from the buckets prior to the change (col 7, lines 43 to col 8, line 33; a statistics database is consulted including a threshold based upon incident rate to determine in part whether or not the event data set should be combined or split. Once a decision is made, variables within the event data set essentially remain the same).

As to claim 66, Lyle teaches the method of claim 63 wherein further comprising comparing accumulated statistic values from the buckets to second threshold values to

determine that an event is of significance (col 7, lines 32-42 and col 8, lines 6-14; many thresholds, such as incident rate, preconfigured criteria, timestamps, etc, are considered in determining the significance or importance of a possible attack)

As to claim 67, Lyle teaches the method of claim 63, wherein comparing statistic values comprises accumulating statistic values from the packets and comparing the values accumulated in the buckets to thresholds that depend on the number of buckets. (col 7, lines 3-20 and 43-67; sniffers are utilized in capturing packet content as well as data related to packets. Thereafter, the data requiring further analysis and/or evaluation is discerned and stored and placed into a queue for further scrutiny by the tracking system).

As to claim 68, Lyle teaches the method of claim 63 wherein the variable number of buckets dynamically adjusts the amount of traffic and number of flows monitored so that the monitoring device is not vulnerable to a denial of service attack against its own resources (col 19, lines 37-45; the protocol disclosed by Lyle teaches a strong protection against denial of service attacks as well as other forms of attacks).

Claim 70 is essentially the computer product residing on a computer readable medium of claim 63 and thus rejected under similar rationale.

Claim 71 is essentially the computer product residing on a computer readable medium of claim 64 and thus rejected under similar rationale.

Claim 72 is essentially the computer product residing on a computer readable medium of claim 65 and thus rejected under similar rationale.

Claim 73 is essentially the computer product residing on a computer readable medium of claim 66 and thus rejected under similar rationale.

Claim 74 is essentially the computer product residing on a computer readable medium of claim 67 and thus rejected under similar rationale.

Claim 75 is essentially the computer product residing on a computer readable medium of claim 68 and thus rejected under similar rationale.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-21, 50-62, 69, and 76-77 rejected under 35 U.S.C. 103(a) as being unpatentable over Lyle further in view of Hsu et al (USPN: 6,098,157) hereinafter referred to as Hsu.

As to claim 1, Lyle teaches a method of monitoring traffic flow in a monitor device disposed to receive network traffic packets comprises:

Producing statistics corresponding to a parameter of traffic flow to trace the source of an attack (Fig 9, 908-310; col 2, lines 45-50; col 7, lines 3-12; sniffers are used in analyzing and evaluating traffic flows to scrutinize suspicious activity in an attempt to ascertain the source of an attack), with producing further comprising:

Mapping the traffic flow into a plurality of buckets (col 7, lines 43-67; event data, which is defined as suspicious data is placed in a queue as a set corresponding to a single incident)

Accumulating statistics from the packets and comparing the number of buckets to a threshold (col 7, lines 32-42 and col 8, lines 6-14; many thresholds, such as incident rate, preconfigured criteria, timestamps, etc, are considered in determining the significance or importance of a possible attack)

Determining whether to vary the number of buckets according to the amount of traffic and number of flows according to down traffic flow into different buckets and examining statistics accumulated for a parameter and a corresponding threshold in the bucket (col 7, line 43 to col 8, line 5; col 13, lines 42-50; once an event (a set of data corresponding to an attack) is placed in the queue, other event data is grouped or combined with existing event data to associate related events into a single incident object. Also, events that do not bear similarities on their face may also be combined or aggregated based upon event rate in a given network or sub-network. Thus varying the amount of event data sets destined for the analysis framework module).

Although Lyle does teach the use of hash functions in a unique way to efficiently communicate with the system (see col 19, lines 11-36), however, Lyle does not explicitly indicate the use of a hash function to output an integer corresponding to one of the buckets.

Hsu teaches a using a hash to output an integer corresponding to the location of a location of a unique bucket identifier (see fig 8, col 4, lines 26-38; col 5, lines 18-23)

It would have been obvious to one with ordinary skill in the art at the time the invention was made to combine the disclosure of Lyle with the hashing techniques in Hsu to make the system more efficient. Using the hashing technique, which utilizes addresses, will output the unique bucket identifier quickly. Because Lyle also uses addresses to relate event data to aggregate events into a single incident object, the use of Hsu's hashing technique would work seamlessly.

As to claim 2, Lyle teaches the method of claim 1 wherein the buckets are storage areas in a memory space (abstract, col 7, lines 46-50; event sets are stored in queues that are also part of the overall memory space of the resident computing device).

As to claim 3, Lyle teaches the method of claim 1 wherein as the number of buckets changes, the buckets have values derived from the buckets prior to change (col 7, liens 59-67 events related to a single incident are combined to produce a single object that has data corresponding with the event database).

As to claim 4, Lyle and Hsu teach the method claim of claim 1 wherein the hash function adapts to map to the new number of buckets, as the new number of buckets changes (col 4, lines 26-38; the bucket identifier is unique and if a bucket is eliminated, so is its corresponding identifier. If, on the other hand, a bucket is added, a unique identifier is created).

As to claim 5, Lyle teaches the method of claim 1, wherein comparing statistic values comprises accumulating statistic values from the packets and comparing the values accumulated in the buckets to thresholds that depend on the number of buckets.

(col 7, lines 3-20 and 43-67; sniffers are utilized in capturing packet content as well as data related to packets. Thereafter, the data requiring further analysis and/or evaluation is discerned and stored and placed into a queue for further scrutiny by the tracking system).

As to claim 6, Lyle teaches the method of claim 1 wherein the parameter is the count of how many packets a data collector or gateway examines (col 7, lines 3-20 and 43-67; sniffers are utilized in capturing packet content as well as data related to packets including the number of packets collected).

As to claim 7, Lyle teaches the method of claim 1 wherein as a value of a parameter approaches a threshold, the monitoring device raises an alarm (see fig 9, col 8, lines 15-53; a policy database is consulted in determining what action should be taken, such a sending alarms)

As to claim 8, Lyle teaches the method of claim 1 wherein the hash function changes periodically in a randomly secret manner so that packets are reassigned to different buckets (Figs 11 A and B)

As to claim 9, Lyle teaches the method of claim 1 wherein the variable number of buckets dynamically adjusts the amount of traffic and number of flows monitored so that the monitoring device is not vulnerable to a denial of service attack against its own resources (col 19, lines 37-45; the protocol disclosed by Lyle teaches a strong protection against denial of service attacks as well as other forms of attacks).

As to claim 10, Lyle teaches the variable number of buckets efficiently identifies the source or sources of attack by breaking down traffic into different buckets and

examining statistics accumulated for a parameter and a corresponding threshold in each bucket (col 8, lines 34-53; the event along with the policy assigned for that event is used in tracking the attack back to its origin, the incident object to which the event was designated would in fact identify the source of the attack).

As to claim 11, Lyle teaches the method of claim 1 wherein the traffic is monitored at multiple levels of granularity, from aggregate to individual flows (col 7, lines 3 to col 8, line 53; individual packets to events to incident objects are analyzed and evaluated at numerous times during processing of given information)

As to claim 12, Lyle teaches the method of claim 1 wherein the method of claim 1 is applied to monitoring of TCP packet rations and repressor traffic (col 7 line 59 to col 8, line 4; traffic from numerous types of networks including tcp/ip based networks is used and numerous values included in the statistics database are disclosed).

As to claim 13, Lyle teaches the method of claim 1 wherein further comprising comparing accumulated statistic values from the buckets to second threshold values to determine that an event is of significance (col 7, lines 32-42 and col 8, lines 6-14; many thresholds, such as incident rate, preconfigured criteria, timestamps, etc, are considered in determining the significance or importance of a possible attack)

Claims 14-21, 50-62 and 76-77 are essentially the computer program product and data collector for the above-mentioned method claims and are thus rejected under similar rationale.

(10) Response to Argument

At the onset, it should be noted that appellant has amended the claims under which there was a 35 USC 112 rejection. This amendment overcomes the rejection and thus it is withdrawn. It should, however, be kept in mind that the rejection was applied prior to appellant's amendment and was proper. It should also be noted that numerous claim limitations argued by the appellant are not present in all independent claims (i.e. the claims are not parallel as some independent claims may not have the argued limitation or it may be presented as a dependent claim).

Appellant argues:

Lyle neither describes nor suggests producing statistics corresponding to a parameter of traffic flow (Argument A-see brief page 10)

In response, the examiner agrees the appellant that "the sniffer 'continuously scans the data being received at various ports of various network devices". Lyle clearly shows the sniffer module is used to monitor network traffic throughout the network and gather information. When the information (statistics) has been gathered and yields a parameter indicating a suspected or actual attack, appropriate action is taken (col 7, lines 7-12 and 32-42). Appellant's claims are broad and thus interpreted as such. The claimed limitation (when present in the set of claims) simply states that "producing *statistics* corresponding to a *parameter* of the traffic flow...". The terms statistic and parameter have not been further defined. Therefore Lyle meets the scope of the limitations as currently claimed.

Furthermore, it should be noted that most of the independent claims do not mention this limitation and if they do, it is presented in the preamble. Conventionally,

such limitations will not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

Appellant further argues:

Lyle does not disclose mapping traffic flow into a plurality of buckets (Argument B-see brief page 11)

In response, the examiner points out that events as described by Lyle's disclosure pertain to traffic flows that correspond to suspicious data. Multiple ports are monitored throughout the network that satisfy a certain pre-configured criteria (col 7, lines 32-42). These traffic flows are placed in events or buckets and are placed in queues for further analysis (col 7, lines 43-58). In light of the above clarification, it should be apparent that all limitations as positively claimed are explicitly and set forth in the Lyle disclosure. Furthermore, the examiner notes that nowhere in the claims, independent or dependent, is there a recitation that the traffic flow must contain an entire set of packets starting from point X and ending at point Y. Therefore, there is no limitation on the size of the flow. It could essentially be a single packet at a port egress or ingress. Therefore Lyle meets the scope of the limitations as currently claimed.

Appellant additionally argues:

Lyle does not describe varying the number of buckets according to the amount of traffic (Argument C-see brief page 11)

In response, the examiner agrees with the appellant that Lyle teaches that events that are not related to any other events are associated with a new incident object. Contrarily, events corresponding to an existing event or group of related events are aggregated or combined into a single event. Furthermore, Lyle teaches that as the traffic increases new events are created to accommodate new incidents. However if the traffic corresponds to an existing event, the events will be combined to save resources. Also, event rates and flows received close in time in the same network are taken into consideration when creating/dividing/aggregating an event (col 13, lines 19-59). Therefore Lyle meets the scope of the limitation as currently claimed.

Appellant further argues:

Lyle does not teach that monitoring device is protected against DoS attacks (Argument D-see brief page 12)

In response, Lyle clearly indicates that its method provides strong protection and is robust against DoS attacks (col 19, lines37-45). Throughout the disclosure, Lyle describes its method as a protocol. For example, in the same column in question (col 19), Lyle describes his method in Figure 11 A and then continues by saying, "The communication protocol described above is advantageous because it..." Similarly, Lyle shows that his method is robust against DoS. So therefore, Lyle disclosure including

the varying of the number of buckets provides the intended protection against DoS attacks.

Appellant additionally argues:

Lyle does not describe that the number of buckets changes based on a comparison to a threshold (Argument E-see brief page 13)

In response, the examiner agrees with the appellant that Lyle teaches that events that are not related to any other events are associated with a new incident object. Contrarily, events corresponding to an existing event or group of related events are aggregated or combined into a single event. Furthermore, Lyle teaches that as the traffic increases new events are created to accommodate new incidents. However if the traffic corresponds to an existing event, the events will be combined to save resources.

At this point, it should be noted that the appellant's claims are broad and interoperated as such. The claimed limitation does not further describe what the threshold is based on, how it is used, etc. In light of this, Lyle teaches the buckets are aggregated/created, divided based on a threshold of how close the incidents relate to one another. Furthermore, event rates and flows received close in time in the same network (yet another threshold) are taken into consideration when creating/dividing/aggregating an event (col 13, lines 19-59). Therefore Lyle meets the scope of the limitation as currently claimed.

Appellant further argues:

One would not be motivated to combine Lyle with Hsu (Argument F-see brief page 18)

It should be noted that Lyle does teach a hashing function. Therefore the system of Lyle is able to properly incorporate hashing. Lyle does however fail in determining an integer by applying a hashing function. Hsu teaches using a hashing function to output an integer corresponding to the location of a unique bucket identifier. The examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). The examiner stated in the previous office action that "[I]t would have been obvious to one with ordinary skill in the art at the time the invention was made to combine the disclosure of Lyle with the hashing techniques in Hsu to make the system more efficient. Using the hashing technique, which utilizes addresses, will output the unique bucket identifier quickly. Because Lyle also uses addresses to relate event data to aggregate events into a single incident object, the use of Hsu's hashing technique would work seamlessly." Therefore, not only does Hsu cure the deficiencies of Lyle but would also be seamlessly incorporated into the teachings of Lyle.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Asad M. Nawaz
Patent Examiner
GAU 2155

Conferees:
Saleh Najjar
Supervisory Patent Examiner
Technology Center 2100

SALEH NAJJAR
SUPERVISORY PATENT EXAMINER

/Lynne H Browne/
Lynne H. Browne
Appeal Practice Specialist, TQAS
Technology Center 2100